10-02-00

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 42390.P8382X Total Pages 4, including fee transmittal

First Named Inventor or Application Identifier Robert W. Faber et al.

Express Mail Label No. EL 627 465 260 US

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. XX Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. XX Specification (Total Pages 24)
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. XX Drawings(s) (35 USC 113) (Total Sheets 4)

4. XX Oath or Declaration (Total Pages 6)

a. XX Newly Executed (Original or Copy)

b. ___ Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**

i. ___ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. __ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. __ Microfiche Computer Program (Appendix)

7. __ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. XX Assignment Papers (cover sheet & documents(s))
9. __ a. 37 CFR 3.73(b) Statement (where there is an assignee)
__ b. Power of Attorney
10. __ English Translation Document (if applicable)
11. XX a. Information Disclosure Statement (IDS)/PTO-1449
XX b. Copies of IDS Citations
12. __ Preliminary Amendment
13. XX Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. __ a. Small Entity Statement(s)
b. Statement filed in prior application, Status still proper and desired
15. __ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. __ Other: _____

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:
___ Continuation ____ Divisional XX Continuation-in-part (CIP)
of prior application No: 09/385,590 filed 8/29/1999 and 09/385,592 filed 8/29/1999

18. **Correspondence Address**
_____ Customer Number or Bar Code Label _____
(Insert Customer No. or Attach Bar Code Label here)
or
X Correspondence Address Below

NAME Michael J. Mallie, Reg. No. 36,591
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
ADDRESS 12400 Wilshire Boulevard
Seventh Floor
CITY Los Angeles STATE California ZIP CODE 90025-1026
Country U.S.A. TELEPHONE (408) 720-8598 FAX (408) 720-9397

Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PTO/SB/17(10/96)
Approved for use through 09/30/98. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL

TOTAL AMOUNT OF PAYMENT ($) 856.00

Complete if Known:

Application No.	Unassigned
Filing Date	September 29, 2000
First Named Inventor	Robert W. Faber
Group Art Unit	Unassigned
Examiner Name	Unassigned
Attorney Docket No.	42390.P8382X

METHOD OF PAYMENT (check one)

1. [ ] **The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:**

   Deposit Account Number _____
   Deposit Account Name _____

   [X] **Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17, charge any deficiencies, and credit any over payments to Deposit Account Number 02-2666**

   [ ] **Charge the Issue Fee Set in 37 CFR 1.18 at the Mailing of the Notice of Allowance, 37 CFR 1.131(b)**

2. X **Payment Enclosed**
   X **Check**
   _____ **Money Order**
   _____ **Other**

FEE CALCULATION (fees effective 10/01/97)

1. **FILING FEE**

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility application filing fee	690.00
106	310	206	155	Design application filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional application filing fee	

SUBTOTAL (1) $ 690.00

2. **CLAIMS**

			Extra		Fee from below		Fee Paid
Total Claims	27	- 20 =	7	X	18.00	=	126.00
Independent Claims	3	- 3 =	0	X	0	=	0
Multiple Dependent Claims				X		=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
103	18	203	9	Claims in excess of twenty	126.00
102	78	202	39	Independent claims in excess of 3	
104	260	204	130	Multiple dependent claim	
109	78	209	39	Reissue independent claims over original patent	
110	18	210	9	Reissue claims in excess of 20 and over original patent	

SUBTOTAL (2) $ 126.00

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for response within first month	
116	380	216	190	Extension for response within second month	
117	870	217	435	Extension for response within third month	
118	1,360	218	680	Extension for response within fourth month	
128	1,850	228	925	Extension for response within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive unavoidably abandoned application	
141	1,210	241	605	Petition to revive unintentionally abandoned application	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	40.00
146	760	246	380	For filing a submission after final rejection (see 37 CFR 1.129(a))	
149	760	249	380	For each additional invention to be examined (see 37 CFR 1.129(a))	

SUBTOTAL (3) $ 40.00

*Reduced by Basic Filing Fee Paid

SUBMITTED BY:

Typed or Printed Name: Michael J. Mallie

Signature _____ Date 9/29/00

Reg. Number 36,591 Deposit Account User ID _____ (complete if applicable)

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EL 627 465 260 US

Date of Deposit: September 29, 2000

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to BOX APPLICATION, Assistant Commissioner for Patents, Washington, D.C. 20231.

Claire Wallters

Name of Person Mailing Paper or Fee

Claire Wallters

Signature of Person Mailing Paper or Fee

September 29, 2000

Date Signed

42390.P8382X *PATENT*

UNITED STATES PATENT APPLICATION

for

METHOD AND APPARATUS FOR AUTHENTICATING AN HIERARCHY OF VIDEO RECEIVING DEVICES

Inventor(s):
Robert W. Faber
Brendan S. Traw
Gary L. Graunke
David A. Lee

prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP
12400 Wilshire Boulevard, 7th Floor
Los Angeles, California 90025
(408)720-8300

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EL 627465260US
Date of Deposit: September 29, 2000
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231

Claire Wallters
(Typed or printed name of person mailing paper or fee)

Claire Wallters
(Signature of person mailing paper or fee)

September 29, 2000
(Date signed)

Method And Apparatus For Authenticating An Hierarchy of Video Receiving Devices

Related Application

This application is a continuation-in-part application to U.S. Patent Applications number 09/385,590 and 09/385,592, both entitled Digital Video Content Transmission Ciphering and Deciphering Method and Apparatus, filed on August 29, 1999.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of content protection. More specifically, the present invention addresses authentication of hierarchically organized video receiving devices.

2. Background Information

In general, entertainment, education, art, and so forth (hereinafter collectively referred to as "content") packaged in digital form offer higher audio and video quality than their analog counterparts. However, content producers, especially those in the entertainment industry, are still reluctant in totally embracing the digital form. The primary reason being digital contents are particularly vulnerable to pirating. As unlike the analog form, where some amount of quality degradation generally occurs with each copying, a pirated copy of digital content is virtually as good as the "gold master". As a result, much effort have been spent by the industry in developing and adopting techniques to provide protection to the distribution and rendering of digital content.

Historically, the communication interface between a video source device (such as a personal computer) and a video sink device (such as a monitor) is an analog interface. Thus, very little focus has been given to providing protection for the transmission between the

source and sink devices. With advances in integrated circuit and other related technologies, a new type of digital interface between video source and sink devices is emerging. The availability of this type of new digital interface presents yet another new challenge to protecting digital video content. While in general, there is a large body of cipher technology known, the operating characteristics such as the volume of the data, its streaming nature, the bit rate and so forth, as well as the location of intelligence, typically in the source device and not the sink device, present a unique set of challenges, requiring a new and novel solution. Parent applications number 09/385,590 and 09/385,592 disclosed various protocol and cipher/deciphering techniques to authenticate a video sink device and protect transmission to the video sink device.

As technology advances, it is desired to be able to securely transmit digital video from a video source device to multiple hierarchically organized video sink devices. Thus, a need exist to authenticate devices and protect transmission in such hierarchical environment.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 illustrates an example hierarchy of video source, repeater and sink devices incorporated with the teachings of the present invention, in accordance with one embodiment;

Figure 2 illustrates an overview of the authentication method of the present invention, in accordance with one embodiment;

Figure 3a illustrates the process for authenticating a video repeater device to a video source device, in accordance with one embodiment (which in one embodiment, is also the same process for authenticating a downstream video repeater device to an upstream video repeater device, a video sink device to a video repeater device, as well as a video sink device to a video source device);

Figure 3b illustrates the process for a video repeater device authenticating downstream video sink devices to an upstream video repeater device or a video source device; and

Figures 4a-4c illustrate a one way function suitable for use to practice the symmetric ciphering/deciphering process employed in one embodiment of the processes illustrated in **Fig. 3a-3b** in further detail, in accordance with one embodiment.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described, and various details will be set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention, and the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention. However, the order of description should not be construed as to imply that these operations are necessarily performed in the order they are presented, or even order dependent. Lastly, repeated usage of the phrase "in one embodiment" does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein a block diagram illustrating an example hierarchy of video source, repeater and sink devices incorporated with the teachings of the present invention for authenticating the downstream video sink devices to the video source device is shown. As illustrated, example hierarchy **100** includes video source device **102**, video sink devices **104a-104d**, and video repeater devices **106a-106b**, coupled to each other as shown. As will be described in more detail below, each video device **102**, **104a-104d** or **106a-106b** includes an authentication unit (not shown) correspondingly incorporated with the applicable aspects of the teachings of present invention for authenticating video sink devices **104a-104d** to video source device **102**, to assure video source device **102** that post authentication video transmitted by video source device **102** will not be compromised by the downstream devices, such as making unauthorized copy of the video.

Except for the teachings of the present invention correspondingly incorporated therein, video source, repeater and sink devices **102**, **104a-104d**, and **106a-106b** are intended

to represent a broad range of digital devices known in the art. For examples, video source **102** may be any one of a number of digital "computing" devices known in the art, including but are not limited to, server computers, desktop computers, laptop computers, set-top boxes, DVD players and the like, and video sink devices **104a-104d** may be, but are not limited to, display devices such as Cathode Ray Tubes (CRT), flat panel displays, television sets, and the like, attached to these digital "computing" devices. Alternatively, one or more video sink devices **104-104d** may be another digital computing device with storage capability or a digital recording device. Video repeater devices **106a-106b** may be, but are not limited to, signal repeater devices.

These devices may be coupled to one another using any one of a number of communication links known in the art. Each of inter-device communication links for conducting the authentication process may or may not be the same communication link for transmitting the post-authentication video signals. In one embodiment, the devices are communicatively coupled to each other using serial communication links known in the art. Communications may be conducted with any pre-established protocols, which are of no particular relevance to the present invention.

Before proceeding to describing the authentication process of the present invention, it should be noted that while for ease of understanding, example hierarchy **100** includes only two repeater devices and four sink devices hierarchically organized into four hierarchy levels, video source device **102**, video sink device **104a** and video repeater device **106a**, video sink devices **104b-104c** and video repeater device **106b**, and video sink device **104d**, from the description to follow, it will be readily apparent to those skilled in the art, that the present invention may be practiced with any number of video repeater and sink devices hierarchically organized in two or more hierarchy levels. Any number of video repeater and sink devices may be present at each level. Further, a video repeater device may also be a video sink device. Nevertheless, for ease of understanding, the remaining description will treat repeater and sink devices as separate devices.

Figure 2 illustrates an overview of the authentication process of the present invention, in accordance with one embodiment. As shown, upon start up, such as power on or reset, at **202**, a downstream video repeater/sink device will first authenticate itself to the immediately upstream video source/repeater device. For example, in the case of example hierarchy **100** of **Fig. 1**, video sink device **104a** and video repeater device **106a** will authenticate itself to video source device **102**, video repeater device **106b** and video sink devices **104b-104c** will authenticate itself to video repeater device **106a**, and video sink device **104d** will authenticate itself to video repeater device **106b**.

For the illustrated embodiment, these authentications are all advantageously conducted with the same authentication process. That is, the operations performed by a pair of video source and sink devices, a pair of video source and repeater devices, a pair of video repeater devices, and a pair of video repeater and sink devices to authenticate the repeater/sink device to the source/repeater device, as the case may be, are basically the same operations. To differentiate an authenticating video repeater device, such as **106a** or **106b**, from a video sink device, such as **104a**, **104b**, or **104c**, a video repeater device, such as **106a** or **106b**, will identify itself to the immediately upstream device, such as device **102a** or **106a**, that the device is a repeater device, and a video sink device, such a **104a-104d** would not make such identification, thereby facilitating the participate devices to know whether the remaining authentication process, to authenticate the downstream video sink devices need to be performed or not.

At **204**, an upstream device, such as source device **102** or repeater device **106a**, will await the downstream device who has identified itself as a repeater device, such as device **106a** and **106b**, to provide the authentication information of all their downstream video sink devices, in the case of repeater device **106a**, sink devices **104b-104c**, and the case of repeater device **106b**, sink devices **104c**. When ready, that is having aggregated all authentication information of the downstream sink devices, repeater device **106a/106b** would perform the

remaining operations authenticating all downstream video sink devices to its immediately upstream device. As examples, in the case of example hierarchy **100** of **Fig. 1**, upon authenticating video sink device **104d**, video repeater device **106b** would authenticate video sink device **104d** to immediately upstream video repeater device **106a**, and for video repeater device **106a**, upon first authenticating video repeater device **106b** and video sink devices **104b-104c**, and then authenticating video sink device **104d**, video repeater device **106a** would authenticate video sink devices **104b-104d** to video source device **102**. In each case, i.e. video repeater device **106b** authenticating video sink device **104d** to video repeater device **106a**, and video repeater device **106a** authenticating video sink devices **104b-104d** to video source device **102**, video repeater device **106a/106b** also provides the topology information of the sink devices to video repeater/source device **106a/102**. In other words, video repeater device **106b** will inform video repeater device **106a** that video sink device **104d** is immediately downstream from it, whereas video repeater device **106a** will inform video source device **102** that video sink devices **104b-104c** are immediately downstream from it, and video sink device **104d** is downstream from it via video repeater device **106b**.

Accordingly, it can be seen, except for practical or commercial reasons, the present invention has no structural limit to the number video sink devices that can be attached to a video repeater device at each hierarchy level, nor is there any structural limit on to the number of hierarchy levels.

In one embodiment, the identical authentication process employed by the devices to authenticate itself to the immediately upstream device, as well as the authentication process employed by a repeater device to authenticate all downstream video sink devices to an immediately upstream video source/repeater device is a cooperative process that involves a symmetric ciphering/deciphering process independently performed by the authentication parties.

Figures 3a-3b illustrate two overviews of the symmetric ciphering/deciphering process based method for authenticating a downstream device to an immediately upstream device, and for a repeater device to authenticate all its downstream sink devices to its immediately upstream device, in accordance with one embodiment. For the illustrated embodiment, all devices correspondingly incorporated with the applicable portions of the teachings of the present invention, video source device **102**, sink devices **104a-104b** and repeater devices **106a-106d**, are assumed to be equipped with an array of "cryptographic" device keys (Akey or Bkey) by a certification authority (hereinafter, simply device keys). In one embodiment, the assignment of these "cryptographic" device keys are performed in accordance with the teachings of the co-pending U.S. Patent Application number 09/275,722, filed on March 24, 1999, entitled Method and Apparatus for the Generation of Cryptographic Keys, having common assignee with the present application.

As illustrated in **Fig. 3a**, the authentication unit of an immediately upstream device, e.g. video source device **102**, video repeater device **106a** or video repeater device **106b**, kicks off the authentication process with each immediately downstream device by generating a basis value (A_n) to the symmetric ciphering/deciphering process, and providing the basis value along with a device key selection vector (A_n, Ak_{sv}) to the immediate downstream device, e.g. video sink device **104a**/video repeater devices **106a**, video repeater device **106b**/video sink devices **104b-104c**, and video sink device **104c**. [Further details on the assignment of device key selection vectors to devices may also be found in the aforementioned application number 09/275,722.] For the example hierarchy **100** of **Fig. 1**, video source device **102** will kick off two authentication processes, one with video sink device **104a** and another one with video repeater device **106a**, video repeater device **106a** will kick off three authentication processes, one with video repeater device **106b** and two others, on each, with video sink device **106b**, and video repeater device **106b** will kick off an authentication process with video sink device **104d**. For the illustrated embodiment, basis

value A_n is a pseudo random number. A_n may be generated in any one of a number of techniques known in the art.

In response, for each of the authentication processes, the authentication unit of the immediately downstream device, e.g. video sink device **104a**/video repeater device **106a**, video repeat device **106b**/video sink devices **104b/104c**, and video sink device **104d** responds by providing its device key selection vector (Bk_{sv}) and an indicator (Repeater) indicating whether the downstream device is a repeater device or not. In one embodiment, the Repeater indicator is a 1-bit indicator set to "1" if the downstream device is a repeater device, and set to "0" if the downstream device is not a repeater device.

Thereafter, for each of the authentication processes, each of the authentication units, of the upstream and downstream devices, will independently generate a verification value R_0 and R_0', using the basis value A_n, their deviec keys, and the exchanged device key selection vectors AK_{sv} and BK_{sv} and the Repeater indicator. The authentication unit of the downstream device will provide its independently generated verification value R_0' to the upstream device, and the authentication unit of the upstream device in turn compares the two verification values, and depending on whether the two verification values successfully compares, uses the provided Bk_{sv} to determine if the downstream device is an authorized device or a device to be trusted. The upstream device accepts Bk_{sv} and uses it to compare against an authorization list to determine whether the downstream device is an authorized or trustworthy device if R_0 equals R_0', otherwise, if R_0 not equals R_0', the downstream device is deemed to be an unauthorized or untrustworthy device. In one embodiment, subsequent video transmissions, if any, would not be passed by the upstream device to the immediately downstream device that failed the authentication process.

For the illustrated embodiment, the authentication unit of the upstream/downstream device independently generates the verification value R_0/R_0' by first generating an authentication key K_m/K_m'. As illustrated, authentication key K_m/K_m' is generated by summing device key Akey/Bkey over device key selection vector BK_{sv}/AK_{sv} (see application

number 09/275,722 for detail). Next, the authentication unit of the upstream/downstream device independently generates the verification value R_0/R_0' using K_m/K_m', Repeater indicator, and A_n). In one embodiment, the authentication unit generates R_0/R_0' employing a "one way function" with K_m/K_m' and Repeater indicator concatenated with A_n.

For the illustrated embodiment, each authentication unit also generates, as part of the process for generating R_0/R_0', a shared secret M_0/M_0' and a session key K_s/K_s'. Shared secret M_0/M_0' is used in the subsequent authentication of the video sink devices downstream to a video repeater device, as well as the protection of the video transmitted posted authentication. Session key K_s/K_s' is used in the protection of the video transmitted posted authentication. Employment of M_0/M_0' and K_s/K_s' to protect the video transmitted post authentication is the subject matters of the parent applications. See the respective applications for details.

At this point, the authentication process is completed between a video source device and a video sink device, and between a video repeater device and a video sink device. For video source device and video repeater device, and for video repeater device and video repeater device, the process continues as illustrated in **Fig. 3b** for the immediately downstream video repeater device to authenticate to the immediately upstream video source/repeater device all downstream video sink devices.

As illustrated, for each upstream device, where the immediately downstream device has identified itself as a repeater device, it awaits for a "Ready" signal from the immediately downstream repeater device, denoting the downstream repeater device has reliably obtained the device key selection vectors of the downstream video sink devices and the downstream repeater device is ready to provide the list of device key selection vectors to the upstream device for authentication. This operation advantageously allows the device key selection vectors of the downstream video sink devices to be successively "percolated" upward through the downstream repeater devices.

Upon having reliably received all the device key selection vectors of the downstream video sink devices (Bk_{sv} list), the downstream repeater device provides the reliably

accumulated Bk_{sv} list to its immediate upstream repeater/source device. For examples, for example hierarchy **100** of **Fig. 1**, video repeater device **106b**, upon reliably obtaining Bk_{sv} of video sink device **104d**, provides the particular Bk_{sv} to video repeater device **106a**. For video repeater device **106a**, upon authenticating Bk_{sv} of video sink devices **104b-104c** and upon reliably provided Bk_{sv} of video sink device **104d** by video repeater device **106b**, it provides Bk_{sv} of all downstream video sink devices, **104d** as well as **104b** and **104c** to video source device **102**.

For the illustrated embodiment, each of the downstream repeater device provides the Bk_{sv} list along with a verification signature (V') and the topology information of the downstream video sink devices. For example, the topological information provided by video repeater device **106a** to video source device **102** denotes to video source device **102** of the fact that video sink device **104d** is actually downstream to video repeater device **106a** through video repeater device **106b**, however, video sink devices **104b-104c** are immediately downstream to video repeater device **106a**.

For the illustrated embodiment, each authentication unit of an immediately downstream video repeater device generates the verification signature V' using a predetermined hash function hashing the Bk_{sv} list, the topology "vector", and the earlier described shared secret M_0'. In one embodiment, the Bk_{sv} list, the topology "vector", and the earlier described shared secret M_0' are concatenated together. The predetermined hash function may be any "secure" hashing function known in the art.

Upon receiving the Bk_{sv} list, the verification signature, and the topology "vector", in like manner, the immediately upstream source/repeater device independently generates its own verification value V. In one embodiment, the immediately upstream source/repeater device independently generates its own verification value V, using the same hash function, the provided Bk_{sv} list, the topology "vector", and its own independently generated shared secret M_0. Upon generating its own verification value V, the immediately upstream source/repeater device compares the two verification values V and V' to determine whether

to accept the provided Bk_{sv} list. In one embodiment, the immediately upstream source/repeater device accepts the provided Bk_{sv} list (when V=V') and compares the list against an authentication list to determine whether the video sink devices are authorized or trustworthy devices, and rejects the provided Bk_{sv} list if V does not equal V'. If the Bk_{sv} list is rejected, the video sink devices are deemed to be unauthorized or untrustworthy sink devices. When that occurs, future video will not be provided to the immediately downstream video repeater device, thereby protecting the video from being sent to the unauthorized or untrustworthy video sink devices.

Figures 4a-4c illustrate a one-way function suitable for use to practice the symmetric ciphering/deciphering process of **Fig. 3a-3b**, in accordance with one embodiment. As alluded to earlier, in one embodiment, this one-way function is a part of the authentication unit of each of the video source/repeater/sink devices. As illustrated in **Fig. 4a**, the one way function **800** includes a number of linear feedback shift registers (LFSRs) **802** and combiner function **804**, coupled to each other as shown. LFSRs **802** and combiner function **804** are collectively initialized with the appropriate keys and data values. During operation, the values are successively shifted through LFSRs **802**. Selective outputs are taken from LFSRs **802**, and combiner function **804** is used to combine the selective outputs to generate the desired outputs.

In one embodiment, four LFSRs of different lengths are employed. Three sets of outputs are taken from the four LFSRs. The polynomials represented by the LFSR and the bit positions of the three sets of LFSR outputs are given by the table to follow:

LFSR	Polynomial	Combining Function Taps		
		0	1	2
3	$X^{17}+x^{15}+x^{11}+x^{5}+1$	5	11	16
2	$X^{16}+x^{15}+x^{12}+x^{8}+x^{7}+x^{5}+1$	5	9	15
1	$X^{14}+x^{11}+x^{10}+x^{7}+x^{6}+x^{4}+1$	4	8	13
0	$X^{13}+x^{11}+x^{9}+x^{5}+1$	3	7	12

The initialization of the LFSRs and the combiner function, more spefically, the shuffling network of the combiner function, is in accordance with the following table.

	Bit Field		Initial Value
LFSR3	[16]		Complement of input bit 47
	[15:0]		Input bits[55:40]
LFSR2	[15]		Complement of input bit 32
	[14:0]		Input bits[39:25]
LFSR1	[13]		Complement of input bit 18
	[12:0]		Input bits[24:12]
LFSR0	[12]		Complement of input bit 6
	[11:0]		Input bits[11:0]
Shuffle Network	Register A		0
	Register B		1

The combined result is generated from the third set of LFSR outputs, using the first and second set of LFSR outputs as data and control inputs respectively to combiner function **804**. The third set of LFSR outputs are combined into a single bit.

Fig. 4b illustrates combiner function **804** in further detail, in accordance with one embodiment. As illustrated, combiner function **804** includes shuffle network **806** and XOR **808a-808b**, serially coupled to each other and LFSRs **802** as shown. For the illustrated embodiment, shuffle network **806** includes four binary shuffle units **810a-810d** serially coupled to each other, with first and last binary shuffle units **810a** and **810d** coupled to XOR **808a** and **808b** respectively. XOR **808a** takes the first group of LFSR outputs and combined them as a single bit input for shuffle network **806**. Binary shuffle units **810a-810d** serially propagate and shuffle the output of XOR **808a**. The second group of LFSR outputs are used to control the shuffling at corresponding ones of binary shuffle units **810a-810d**. XOR **808b** combines the third set of LFSR outputs with the output of last binary shuffle unit **810d**.

Fig. 4c illustrates one binary shuffle unit **810*** (where * is one of **a-d**) in further detail, in accordance with one embodiment. Each binary shuffle unit **810*** includes two flip-flops **812a** and **812b**, and a number of selectors **814a-814c**, coupled to each other as shown. Flip-flops **812a** and **812b** are used to store two state values (A, B). Each selector **814a**, **814b** or **814c** receives a corresponding one of the second group of LFSR outputs as its control signal. Selector **814a-814b** also each receives the output of XOR **808a** or an immediately preceding binary shuffle unit **810*** as input. Selector **814a-814b** are coupled to flip-flops **812a-812b** to output one of the two stored state values and to shuffle as well as modify the stored values in accordance with the state of the select signal. More specifically, for the illustrated embodiment, if the stored state values are (A, B), and the input and select values are (D, S), binary shuffle unit **810*** outputs A, and stores (B, D) if the value of S is "0". Binary shuffle unit **810*** outputs B, and stores (D, A) if the value of S is "1".

Accordingly, a novel method and apparatus for authenticating hierarchically organized video repeater and sink devices has been described.

Epilogue

From the foregoing description, those skilled in the art will recognize that many other variations of the present invention are possible. Thus, the present invention is not limited by the details described, instead, the present invention can be practiced with modifications and alterations within the spirit and scope of the appended claims.

CLAIMS

What is claimed is:

1. A method comprising:

a video source device and a first video repeater device cooperatively authenticating the first video repeater device to the video source device;

the first video repeater device and first at least one video sink device cooperatively and correspondingly authenticating the first at least one video sink device to the first video repeater device; and

the video source device and the first video repeater device cooperatively authenticating the first at least one video sink device to the video source device.

2. The method of claim 1, wherein said cooperative authentication of the first video repeater device to the video source device comprises said video source device and said first video repeater device employing an identical authentication protocol said video source device and a video sink device would employ to authenticate said video sink device to said video source device, and augmenting said identical authentication protocol with identification of said first video repeater device as a repeater device to said video source device.

3. The method of claim 1, wherein said cooperative authentication of the first video repeater device to the video source device comprises

said video source device and said first video repeater device exchanging device key selection vectors with each other;

said first video repeater device identifying itself as a repeater device to said video source device;

said first video repeater device providing said video source device with a verification key generated using a symmetric ciphering process with an authentication key generated using the received device key selection vector of said video source device; and

said video source device verifying said verification key provided by said first video repeater device.

4. The method of claim 3, wherein said cooperative authentication of the first video repeater device to the video source device further comprises said first video repeater device generating said authentication key using said received device key selection vector of said video source device and its own device key.

5. The method of claim 1, wherein

said cooperative authentication of the first video repeater device to the video source device comprises said video source device and said first video repeater device exchanging device key selection vectors with each other; and

said method further comprises said video source device and said first video repeater device each independently generating a shared secret using a symmetric ciphering process using an authentication key generated using said device key selection vectors of said video source device and said first video repeater device.

6. The method of claim 1, wherein said cooperative authentication between said first video repeater device and said video source device of the at least one video sink device to the video source device comprises

said first video repeater device providing a device key selection vector of each of said first at least one video sink device, and a verification signature generated using the provided device key selection vector/selection vectors and a shared secret value between said video source device and said first video repeater device; and

said video source device verifying said verification signature.

7. The method of claim 6, wherein said method further comprises said video source device and said first video repeater device each independently generating said shared secret value using a symmetric ciphering process with an authentication key generated based on device key selection vector of said video source device and said first video repeater device.

8. The method of claim 1, wherein

said method further comprises said video source device and a video sink device cooperatively authenticating said video sink device to said video source device;

both of said cooperative authentication of said first video repeater device and said video sink device to said video source device employing an identical authentication protocol, with said cooperative authentication of said first video repeater device to said video source device augmenting said identical authentication protocol with said first video repeater device identifying itself as a repeater device to said video source device.

9. The method of claim 1, wherein said method further comprises

said first video repeater device and a second video repeater device cooperatively authenticating second at least one video sink device to said first video repeater device; and

said video source device and said first video repeater device cooperatively authenticating said second at least one video sink device to said video source device.

10. The method of claim 9, wherein said video source device and said first video repeater device cooperatively authenticating said first and second at least one video sink device to said video source device at the same time.

11. The method of claim 9, wherein said method further comprises said first video repeater conveying topological information of said first and second at least one video sink device to said video source device.

12. In a first video repeater device, a method comprising:

in cooperation with a video source device, authenticating itself to a video source device;

correspondingly in cooperation with at least one video sink device, authenticating first at least one video sink device to said first video repeater device; and

in cooperation with a video source device, authenticating the first at least one video sink device to the video source device.

13. The method of claim 12, wherein said cooperative authentication of the first video repeater device to the video source device comprises said first video repeater device employing an identical authentication protocol a video sink device would employ to authenticate said video sink device to said video source device, and augmenting said identical authentication protocol with identification of said first video repeater device as a repeater device to said video source device.

14. The method of claim 12, wherein said cooperative authentication of the first video repeater device to the video source device comprises

exchanging device key selection vector with said video source device;

identifying said first video repeater device as a repeater device to said video source device; and

providing said video source device with a verification key generated using a symmetric ciphering process with an authentication key generated using the received device key selection vector of said video source device.

15. The method of claim 14, wherein said cooperative authentication of the first video repeater device to the video source device further comprises generating said authentication key using said received device key selection vector of said video source device and its own device key.

16. The method of claim 12, wherein

said cooperative authentication of the first video repeater device to the video source device comprises exchanging device key selection vector with said video source device; and

said method further comprises independently generating a shared secret with said video source device using a symmetric ciphering process using an authentication key generated using said device key selection vector of said video source device and said first video repeater device.

17. The method of claim 12, wherein said cooperative authentication of the at least one video sink device to the video source device comprises providing a device key selection vector of each of said first at least one video sink device, and a verification signature generated using the provided device key selection vector/selection vectors and a shared secret value with said video source device.

18. The method of claim 17, wherein said method further comprises independently generating said shared secret value using a symmetric ciphering process with an authentication key generated based on device key selection vectors of said video source device and said first video repeater device.

19. The method of claim 12, wherein said method further comprises

a second video repeater device in cooperation with said first video repeater device authenticating second at least one video sink device to said first video repeater device; and

in cooperation with said video source device, authenticating said second at least one video sink device to said video source device.

20. The method of claim 19, wherein said first and second at least one video sink devices are authenticated to said video source device at the same time.

21. The method of claim 19, wherein said method further conveying topological information of said first and second at least one video sink device to said video source device.

22. A video repeater apparatus comprising:

first communication interface to couple first at least one video sink device to said video repeater apparatus to exchange first authentication information with the at least one video sink device;

second communication interface to couple the video repeater apparatus to a video source device to first exchange second, then third authentication information to said video source device for first authenticating said video repeater apparatus, then said first at least one video sink device to said video source device; and

an authentication unit coupled to said first and second communication interfaces to authenticate said first at least one video sink device, and to generate the portions of said second and third authentication information of said video repeater apparatus and said first at least one video sink device to be provided to said video source device.

23. The apparatus of claim 22, wherein

said first, second and third authentication information exchanged comprise corresponding pair-wise combinations of device key selection vectors of said video repeater apparatus, said at least one video sink device, and said video source device, with said second and third authentication information further comprising corresponding verification keys, and said second authentication information further comprising information identifying said video repeater apparatus as a video repeater device; and

said authentication unit comprises a ciphering unit to symmetrically generate said verification keys with corresponding authentication keys generated using the corresponding pair-wise combinations of the device key selection vectors.

24. The apparatus of claim 23, wherein said ciphering unit further independently generates corresponding shared secrets between said video repeater apparatus and said at least one video sink device, and between said video repeater apparatus and said video source device using corresponding ones of said authentication keys.

25. The apparatus of claim 24, wherein said ciphering unit further generates said verification keys using corresponding ones of said shared secrets.

26. The apparatus of claim 12, wherein

said first communication interface is to further exchange fourth authentication information of second at least one video sink device with another video repeater apparatus;

said third authentication information is also for authenticating said second at least one video sink device to said video source device.

27. The apparatus of claim 26, wherein said third authentication information further comprises topological information of said first and second at least one video sink device.

ABSTRACT OF THE DISCLOSURE

A video source device and a video repeater device cooperatively authenticates said video repeater apparatus to said video source device. In one embodiment, the authentication is performed using an identical authentication process a video sink device would authenticate itself to the video source device. The video repeater device augment the identical process identifying itself as a repeater device. The video repeater device also in cooperation with at least one video sink device authenticates the at least one video sink device. The video repeater device in turn, in cooperation with the video source device, authenticates the at least one video sink device to the video source device. In one embodiment, the video repeater device also in cooperation with another video repeater device, authenticates yet another at least one video sink device to the video repeater device. In like manner, the video repeater device, in cooperation with the video source device, authenticates the yet another at least one video sink device to the video source device. In one embodiment, the video repeater device includes topological information of the video sink devices among the authentication information provided to the video source device. Accordingly, video sink devices may be hierarchically organized to the video source device.

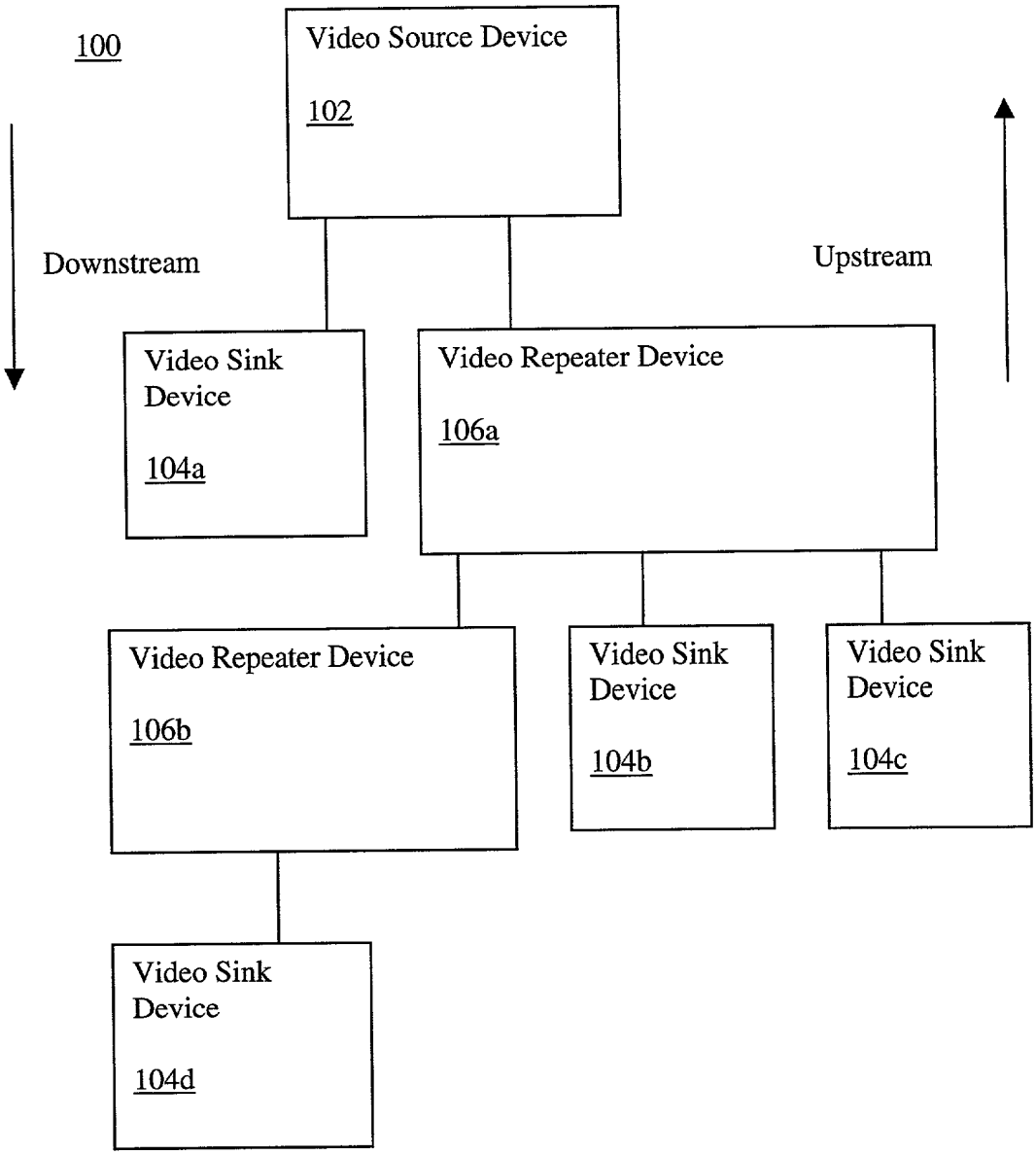
100
Video Source Device
102
Downstream
Upstream
Video Sink Device
104a
Video Repeater Device
106a
Video Repeater Device
106b
Video Sink Device
104b
Video Sink Device
104c
Video Sink Device
104d

Figure 1

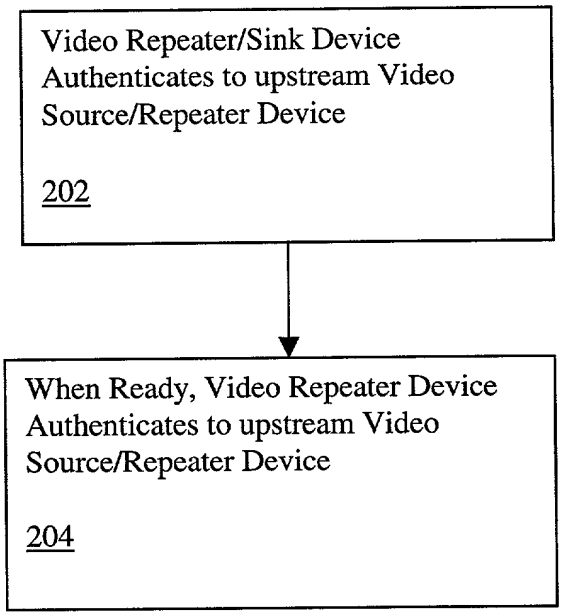
Video Repeater/Sink Device Authenticates to upstream Video Source/Repeater Device
202
When Ready, Video Repeater Device Authenticates to upstream Video Source/Repeater Device
204

Figure 2

Upstream Device		Downstream Device
Video Source/Repeater Device (Ak_{sv})		Video Repeater/Sink Device (Bk_{sv})
Generate A_n	A_n, Ak_{sv} → ← Bk_{sv}, Repeater	
Generate K_m ($Akey_{sv}$, Bk_{sv}) Generate K_s, M_0, R_0 (K_m, Repeater || A_n)		Generate K_m' ($Bkey$, Ak_{sv}, ~~Bk_{sv}~~) Generate K_s', M_0', R_0' (K_m', Repeater || A_n)
Determine if $R_0 = R_0'$	← R_0'	

Figure 3a

Upstream Device		Downstream Device
Video Source/Repeater Device		Video Repeater Device
Poll Ready	← Ready ← KSV list, V', Topology	Assemble KSV list V'=SHA-1(KSV list || Topology || M_0')
V=SHA-1(KSV list || Topology || M_0') Determine if V=V'		

Figure 3b

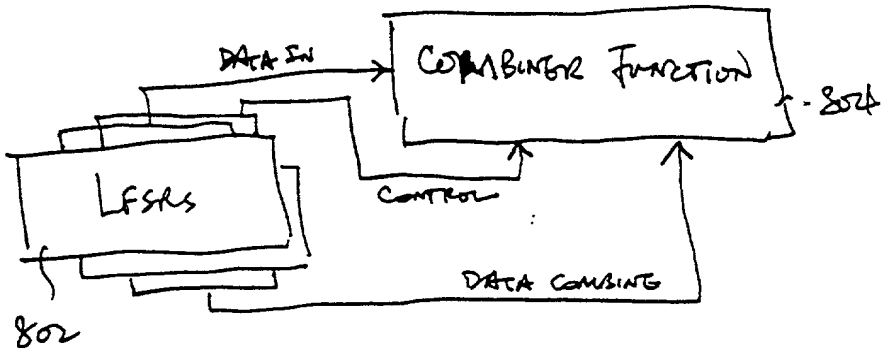

Fig. 4a

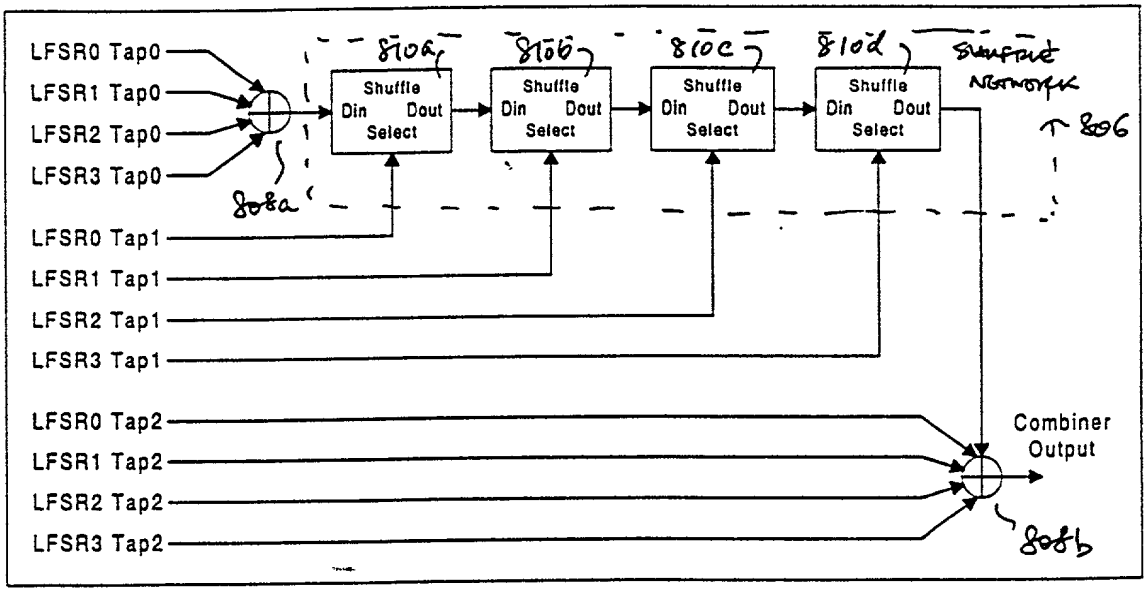

Fig. 4b

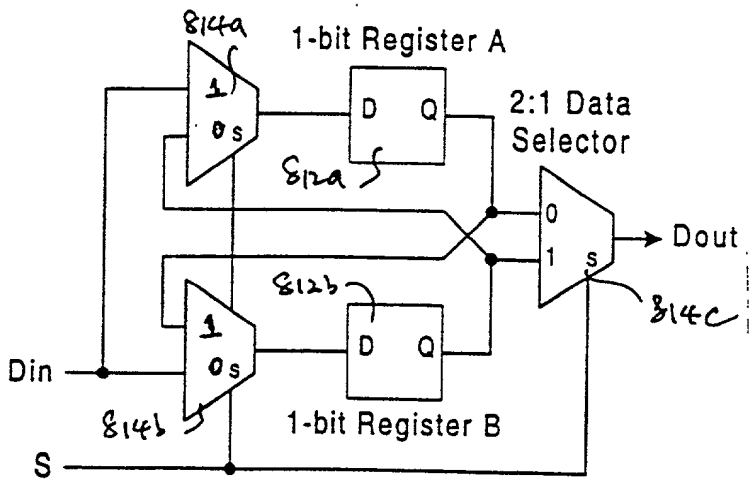

Fig. 4c

Attorney's Docket No.: 42390.P8382X PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR **INTEL CORPORATION** PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND APPARATUS FOR AUTHENTICATING AN HIERARCHY OF VIDEO RECEIVING DEVICES

the specification of which

xx is attached hereto.
___ was filed on _____ as
United States Application Number _____
or PCT International Application Number_____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

Application Number	Filing Date
Application Number	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

09/385,590	8/29/1999	Pending
Application Number	Filing Date	Status -- patented, pending, abandoned
09/385,592	8/29/1999	Pending
Application Number	Filing Date	Status -- patented, pending, abandoned

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to James H. Salter **(Name of Attorney or Agent)**, **BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to** James H. Salter **(Name of Attorney or Agent)**, **(408) 720-8300.**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Robert W. Faber

Inventor's Signature Robert W. Faber Date 22 SEPTEMBER 2000

Residence Hillsboro, Oregon (City, State) Citizenship United States Of America (Country)

Post Office Address 942 NE Third Avenue, Hillsboro, Oregon 97124

Full Name of Second/Joint Inventor Brendan S. Traw

Inventor's Signature CRSTraw Date 9/28/00

Residence Portland, Oregon (City, State) Citizenship United States Of America (Country)

Post Office Address 10859 NW Supreme Court, Portland, Oregon 97229

Full Name of Third/Joint Inventor Gary L. Graunke

Inventor's Signature Gary L Graunke Date 9/28/2000

Residence Hillsboro, Oregon (City, State) Citizenship United States Of America (Country)

Post Office Address 362 NE Hillwood Drive, Hillsboro, Oregon 97124

Full Name of Fourth/Joint Inventor David A. Lee

Inventor's Signature _____ Date 9/26/00

Residence Beaverton, Oregon (City, State) Citizenship United States Of America (Country)

Post Office Address 740 SW Willow Creek Drive
Beaverton, Oregon 97006

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Lisa N. Benado, Reg. No. 39,995; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, Reg. No. P46,503; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George Fountain, Reg. No. 37,374; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; Libby N. Ho, Reg. No. P46,774; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; George Brian Leavell, Reg. No. 45,436; Kurt P. Leyendecker, Reg. No. 42,799; Gordon R. Lindeen III, Reg. No. 33,192; Jan Carol Little, Reg. No. 41,181; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Kenneth B. Paley, Reg. No. 38,989; Marina Portnova, Reg. No. P45,750; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Tom Van Zandt, Reg. No. 43,219; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Firasat Ali, Reg. No. 45,715; and Justin M. Dillon, Reg. No. 42,486; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Edward R. Brake, Reg. No. 37,784; Ben Burge, Reg. No. 42,372; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Peter Lam, Reg. No. 44,855; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Gene I. Su, Reg. No. 45,140; Calvin E. Wells, Reg. No. P43,256, Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.